UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/640,122 | 08/16/2000 | James M. Dunn | 6169-135 | 4634 |

40987 7590 12/22/2004

AKERMAN SENTERFITT
P. O. BOX 3188
WEST PALM BEACH, FL 33402-3188

| EXAMINER | |
|---|---|
| PARTHASARATHY, PRAMILA | |
| **ART UNIT** | **PAPER NUMBER** |
| 2136 | |

DATE MAILED: 12/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/640,122 | DUNN ET AL. | |
| | Examiner | Art Unit | |
| | Pramila Parthasarathy | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *29 June 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☑ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## *DETAILED ACTION*

**1.** This action is in response to request for reconsideration filed on June 29, 2004. Original application contained Claims 1 – 36. Applicant has not canceled any claims. Applicant has amended claims 1 – 5, and 19 – 23. Applicant has new claims 37 – 41. Therefore, presently pending claims are 1 – 41.

## *Response to Arguments*

**2.** Applicant's arguments filed on June 29, 2004, have been fully considered but they are not persuasive for the following reasons:

## *Claim Objections*

**3.** Claim 40 is objected to because of the following informalities:

Replace "with" by "which", Claim 40 line 6.

Appropriate correction is required.

## *Claim Rejections - 35 USC § 112*

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

**4.** Claims 1 – 41 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent and new Claims 1 and 19 read, " ... prompting said user for a combination of obscuring data and the authorizing data, ..... repudiating the obscuring data ....", and Claim 40 reads "A system for secure entry of authorizing data ... and obscuring data ... an authorizing engine ...".

With respect to "obscuring data", although the specification discloses the system can prompt the user for PIN and ATM can compute a obscuring number using obscuring number generation techniques and the user can be prompted to key in the obscuring number, the specification does not disclose a method for obtaining or prompting for obscuring data. The specification does not indicate how the data used to obscure the authorizing data. Applicant amendment does not clarify the steps of obscuring data and directs to specification at page 15 line 22 line – page 16 line 13, page 18 line 16 – page 19 line 7 and page 19 lines 21 – 28, which do not disclose obscuring the authorizing data.

With respect to "repudiating", the specification does not indicate how to perform the step of repudiating the obscuring data during the authorizing step anywhere in the

specification. Applicant remarks/arguments do not address "repudiating the obscuring data during authorization step".

With respect to "authorizing engine", the specification does not disclose how an authorizing engine is configured to authorize use of the publicly positioned device. Authorizing engine is not disclosed in the specification.

The dependent claims 2 – 18, 20 – 39 and 40 are rejected at least by virtue of their dependency on the dependent claims.

Applicant agrees with the Examiner that the cited prior arts (CPA) [Naik et al. U.S. Patent 5,548,647, hereinafter "Naik", Watkins U.S. Patent 5,719,560, hereinafter "Watkins" and Coteus et al. U.S. Patent 5,614,920, hereinafter "Coteus"], disclose a security system that confirms a user's identity thus preventing unauthorized users from gaining access to the secured device and also that CPA teaches prompting for an authorizing data. . Naik discloses a method for ascertaining the identity of user and relates technique for verifying the identity of the user, Watkins discloses a method of automatic verification of personal identity by generating obscuring data and Coteus discloses an apparatus for masking a displayed data by merging it with another image and also an electronic shutter timed to match the sequence of the masking light pulses separates or blocks the masking image to permit the authorizing data to be viewed only by the person having access to the system.

Regarding currently amended claims 1 and 19, Applicant argues that the CPA do not teach "prompting for obscuring data" and "obscuring data that is discarded for

authorizing purposes". These arguments are not found persuasive. Naik discloses, "prompting for obscuring data" (Naik Column 4 lines 27 – 50) and "obscuring data that is discarded for authorizing purposes" (Naik Column 5 lines 15 – 21).

Regarding currently amended claims 4 and 22, Applicant argues that the CPA do not teach, "prompting for obscuring data that is repudiated during an authorizing step". This argument is not found persuasive. Naik discloses, "prompting for obscuring data that is repudiated during an authorizing step" (Naik Column 4 lines 27 – 50 and Column 5 lines 15 - 21) and Watkins discloses "a visual interface for prompting for obscuring data" (Watkins Column 11 lines 60 – 65 and Column 12 lines 44 – 60).

Regarding claims 6 - 15 and 24 - 36, Applicant argues that the CPA do not teach "prompting for obscuring data and then repudiating received obscuring data during an authorizing step". This argument is not found persuasive. Naik discloses, "prompting for obscuring data" (Naik Column 4 lines 27 – 50) and "obscuring data that is discarded for authorizing purposes" (Naik Column 5 lines 15 – 21), Watkins discloses "a visual interface for prompting for obscuring data" and Coteus discloses an apparatus for masking a displayed data by merging it with another image and also an electronic shutter timed to match the sequence of the masking light pulses separates or blocks the masking image to permit the authorizing data to be viewed only by the person having access to the system (Coteus Column 2 lines 30 – 55)

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter "prompting a user for obscuring data then repudiating received obscuring data during an authorizing step" broadly recited in the amended independent claims 1 and 19 and the new independent claim 40. The dependent claims 2 – 18, 20 – 39 and 40 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims 1 – 41 is respectfully maintained.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**5.** Claims 1 – 3, 5, 16 – 21, 23, 37 – 40 and 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Naik et al. (U.S. Patent 5,548,647).

Regarding Claim 1, Naik teaches and describes, a method for secure entry of a authorizing data in a publicly positioned device comprising the stops of:

establishing a private communications link between a user and the publicly positioned device (Fig.1 and Column 4 lines 27 – 50);

prompting said user for a combination of obscuring data and the authorizing data (Column 5 lines 7 – 28);

authorizing the user to utilize the publicly positioned device based upon the authorizing data (Column 8 line 39 – Column 9 line 6); and

repudiating the obscuring data during the authorizing step (Column 5 lines 15 – 21).

Regarding Claim 19, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, said computer program having a plurality of code sections executable by a machine for causing the machine to perform the steps of:

establishing a private communications link between a user and the publicly positioned device (Fig.1 and Column 4 liens 27 – 50);

prompting said user for a combination of obscuring data and the authorizing data (Column 5 lines 7 – 28);

authorizing the user to utilize the publicly positioned device based upon the authorizing data (Column 8 line 39 – Column 9 line 6); and

repudiating the obscuring data during the authorizing step (Column 5 lines 15 – 21).

Regarding Claim 40, Naik teaches and describes, a system for secure entry of authorizing data in a publicly positioned device comprising:

a publicly positioned input device configured to prompt a user for authorizing data and obscuring data (Column 5 lines 7 – 28);

a communication link between the publicly positioned input device and the authorizing engine through which the authorizing data is conveyed (Column 4 lines 27 – 50);

an authorizing engine configured to authorize use of the publicly positioned device based upon the authorizing data, wherein the obscuring data is not used by the authorizing engine to authorize use of the publicly positioned device (Column 8 line 39 – Column 9 line 6).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein: said prompting step comprises the steps of:

separately prompting said user for said obscuring data and authorizing data (Column 5 lines 22 – 26);

combining said obscuring data and the authorizing data into said combination (Column 2 lines 10 – 22).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein: said prompting step comprises the steps of:

dividing the authorizing data into at least two portions (Column 6 lines 10 – 17);

separately prompting said user for each portion of the authorizing data (Column 5 liens 22 – 26 and Column 6 liens 10 – 29) and

prompting said user for authorizing data in between said separate prompts for said at least two portions (Column 6 lines 10 – 29).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein: the publicly positioned device has a telephone interface through which said user can be audibly prompted for said obscuring data and the authorizing data (Fig.1)

Claim 37 is rejected as applied above in rejecting claim 1. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, further comprising the steps of:

before the authorizing step, conveying authorizing data from an input device to an authorizing engine, wherein the obscuring data is not conveyed from the input device to the authorizing engine (Column 5 lines 15 – 21).

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said prompting step comprises the steps of:

separately prompting said user for said obscuring data and the authorizing data (Column 5 lines 22 –26); and,

combining said obscuring data and the authorizing data into said combination (Column 2 lines 10 – 22).

Claim 21 is rejected as applied above in rejecting claim 19. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said prompting step comprises the steps of:

dividing the authorizing data into at least two portions (Column 6 lines 10 –17);

separately prompting said user for each portion of the authorizing data (Column 5 lines 22 – 26 and Column 6 liens 10 – 29);

prompting said user for obscuring data in between said separate prompts for said at least two portions (Column 6 liens 10 – 29); and,

discarding said obscuring data and combining said at least two portions, wherein the authorizing data comprises a combination of said at least two portions (Column 5 lines 15 – 21).

Claim 23 is rejected as applied above in rejecting claim 19. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said prompting step comprises the steps of: the publicly positioned device has a telephone interface through which said user can be audibly prompted for said obscuring data and the authorizing data (Fig.1).

Claim 41 is rejected as applied above in rejecting claim 40. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein the authorizing engine is remotely located from the publicly positioned input device, and wherein the communication link includes a network connection (Fig. 1 and Column 4 line 27 – 61).

Claim 16 is rejected as applied above in rejecting claim 3. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said establishing step comprises the step of:

connecting said user to a telephone operator system through said telephone interface (Column 4 lines 40 – 50),

said prompts audibly provided by said telephone operator system to said user through said telephone interface (Column 4 lines 51 – 62).

Claim 38 is rejected as applied above in rejecting claim 37. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly

positioned device, wherein the authorizing engine is remotely based from the input device (Column 5 lines 37 – 46).

Claim 39 is rejected as applied above in rejecting claim 38. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device further comprising the step of:

encoding the authorizing data before conveying the authorizing data to the authorizing engine (Column 6 lines 10 – 41)

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said telephone operator system is an interactive (Column 6 lines 43 – 62).

Claim 18 is rejected as applied above in rejecting claim 16. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said telephone operator system is a human telephone operator (Column 4 line 27 – Column 5 line 47).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**6. Claims 4 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naik et al. (U.S. Patent 5,548,647) in view of Watkins (U.S. Patent 5,719,560, herein after "Watkins").**

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein: the publicly positioned device has an interface through which said user can be visually prompted for said obscuring data and the authorizing data.

Naik does not teach that the publicly positioned device has a visual interface through which said user can be visually prompted for said obscuring data and the authorizing data. However, Watkins discloses that the publicly positioned device has a visual interface through which said user can be visually prompted for said obscuring data and the authorizing data (Watkins Column 11 lines 60 – 65 and Column 12 lines 44 – 60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine a method for implementing a visual interface through which user can be visually prompted for obscuring data and the authorizing data as taught by Watkins to provide a secure, selective viewing of information, as

taught by Naik, on a display that can easily be enabled by the viewer. The motivation would have been to enhance the level of security of methods of verification of the identity of the user, thereby enhance a speaker verification system and method.

Claim 22 is rejected as applied above in rejecting claim 19. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein: the publicly positioned device has an interface through which said user can be visually prompted for said obscuring data and the authorizing data.

Naik does not teach that the publicly positioned device has a visual interface through which said user can be visually prompted for said obscuring data and the authorizing data. However, Watkins discloses that the publicly positioned device has a visual interface through which said user can be visually prompted for said obscuring data and the authorizing data (Watkins Column 11 lines 60 – 65 and Column 12 lines 44 – 60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine a method for implementing a visual interface through which user can be visually prompted for obscuring data and the authorizing data as taught by Watkins to provide a secure, selective viewing of information, as taught by Naik, on a display that can easily be enabled by the viewer. The motivation would have been to enhance the level of security of methods of verification of the identity of the user, thereby enhance a speaker verification system and method.

**7. Claims 6 – 15 and 24 - 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naik et al. (U.S. Patent 5,548,647) in view of watkins (5,719,560) and further in view of Coteus et al. (U.S. Patent 5,614,920, herein after "Coteus").**

Claim 6 is rejected as applied above in rejecting claim 4. Furthermore, Naik teaches and describes a method for secure entry of an authorizing data in a publicly positioned device. Even when taken together, Naik and Watkins do not teach linking the publicly positioned device through an encoder application to active glasses having a shuttered display, said shuttered display opening and closing responsive to synchronization pulses; synchronizing display of said prompts in said visual interface with said opening and closing of said shuttered display in said active glasses; and, displaying masking data in said visual interface between said display of said prompts.

However, Coteus teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said establishing step comprises:

linking the publicly positioned device through an encoder application to active glasses having a shuttered display, said shuttered display opening and closing responsive to synchronization pulses (Coteus Column 2 lines 30 – 38);

synchronizing display of said prompts in said visual interface with said opening and closing of said shuttered display in said active glasses (Coteus Column 2 lines 32 – 45); and,

displaying masking data in said visual interface between said display of said prompts (Coteus Column 2 lines 46 – 55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine a method for implementing a visual interface through which user can be visually prompted for obscuring data and the authorizing data as taught by Watkins to provide a secure, selective viewing of information, as taught by Naik, on a display that can easily be enabled by the viewer and masking data to permit image to be viewed only by the person having the electronic shutter. The motivation would have been to enhance the level of security of methods of verification of the identity of the user, thereby enhance a speaker verification system and method that can be easily enabled or disabled by the viewer.

Claim 24 is rejected as applied above in rejecting claim 22. Furthermore, Naik teaches and describes a method for secure entry of an authorizing data in a publicly positioned device. Even when taken together, Naik and Watkins do not teach linking the publicly positioned device through an encoder application to active glasses having a shuttered display, said shuttered display opening and closing responsive to synchronization pulses; synchronizing display of said prompts in said visual interface with said opening and closing of said shuttered display in said active glasses; and, displaying masking data in said visual interface between said display of said prompts.

However, Coteus teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said establishing step comprises:

linking the publicly positioned device through an encoder application to active glasses having a shuttered display, said shuttered display opening and closing responsive to synchronization pulses (Coteus Column 2 lines 30 – 38);

synchronizing display of said prompts in said visual interface with said opening and closing of said shuttered display in said active glasses (Coteus Column 2 lines 32 – 45); and,

displaying masking data in said visual interface between said display of said prompts (Coteus Column 2 lines 46 – 55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine a method for implementing a visual interface through which user can be visually prompted for obscuring data and the authorizing data as taught by Watkins to provide a secure, selective viewing of information, as taught by Naik, on a display that can easily be enabled by the viewer and masking data to permit image to be viewed only by the person having the electronic shutter. The motivation would have been to enhance the level of security of methods of verification of the identity of the user, thereby enhance a speaker verification system and method that can be easily enabled or disabled by the viewer.

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said synchronizing step comprises the steps of:

generating a sequencing pattern containing synchronization pulses (Coteus Column 2 lines 1 – 5);

generating a data signal, said data signal comprising private data and masking data frames interspersed according to said sequencing pattern, said private data comprising said prompts:

providing said data signal to said visual interface (Coteus Fig.1 #18 and Column 2 lines 30 – 44); and,

opening and closing said shuttered display in said active glasses in accordance with said sequencing pattern (Coteus Column 2 lines 3 – 13),

whereby said user viewing said visual interface with said active glasses can view said prompts and unauthorized viewers without said active glasses can view only said prompts obscured by said masking data (Coteus Column 3 lines 55 – 61).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said synchronizing step comprises the steps of:

generating a sequencing pattern containing synchronization pulses (Coteus Column 2 lines 1 – 5);

generating a data signal, said data signal comprising private data and masking data frames interspersed according to said sequencing pattern, said private data comprising said prompts:

providing said data signal to said visual interface (Coteus Fig.1 #18 and Column 2 lines 30 – 44); and,

opening and closing said shuttered display in said active glasses in accordance with said sequencing pattern (Coteus Column 2 lines 3 – 13),

whereby said user viewing said visual interface with said active glasses can view said prompts and unauthorized viewers without said active glasses can view only said prompts obscured by said masking data (Coteus Column 3 lines 55 – 61).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Naik teaches and describes a method for secure entry of an authorizing data in a publicly positioned device, wherein said sequencing pattern is encoded (Coteus Column 2 lines 3 – 5 and Column 3 lines 7 – 15).

Claim 9 is rejected as applied above in rejecting claim 7. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said step of generating a data signal comprises the steps of:

inserting masking data in said data signal (Coteus Column 2 lines 56 – 62); and,

inserting said private data in said data signal when indicated by said synchronization pulses in said sequencing pattern (Coteus Column 3 lines 10 – 16 and 45 – 51).

Claim 10 is rejected as applied above in rejecting claim 7. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said step of generating a data signal comprises the step of:

inserting masking data in said data signal (Coteus Column 2 lines 56 – 62); and,

for private data forming a complete character or image, repeatedly inserting portions of said complete character or image when indicted by said synchronization pulses in said sequencing pattern until all portions of said complete character or image are inserted in said data signal (Coteus Column 3 lines 10 – 16 and 45 – 51),

whereby display of said data signal, as viewed by said active glasses synchronized with said interface according to said sequencing pattern is a strobe display of said complete character or image (Coteus Column 2 lines 59 – 67).

Claim 11 is rejected as applied above in rejecting claim 7. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said step of opening and closing said shuttered display comprises the step of, responsive to synchronization pulses in said sequencing pattern, opening and closing said shuttered display (Coteus Column 6 lines 43 – 62).

Claim 13 is rejected as applied above in rejecting claim 7. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said sequencing pattern corresponds to alternating displays of said private data and said masking data (Coteus Column 3 lines 45 – 51).

Claim 14 is rejected as applied above in rejecting claim 7. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said sequencing pattern corresponds to combined left eye/right eye images of said private data (Coteus Column 2 lines 62 - Column 3 line 16).

Claim 15 is rejected as applied above in rejecting claim 7. Furthermore, Naik teaches and describes a method for secure entry of an authorizing data in a publicly positioned device, wherein said masking data is a fill pattern (Coteus Column 2 34 – 40 and 55 – 59).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said sequencing pattern is encoded (Coteus Column 2 lines 3 – 5 and Column 3 lines 7 – 15).

Claim 27 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer

program for secure entry of a authorizing data in a publicly positioned device, wherein said step of generating a data signal comprises the step of:

inserting masking data in said data signal (Coteus Column 2 lines 56 – 62); and,

inserting said private data in said data signal when indicated by said synchronization pulses in said sequencing pattern (Coteus Column 3 lines 10 – 16 and 45 – 51).

Claim 28 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said step of generating a data signal comprises the steps of:

inserting masking data in said data signal (Coteus Column 2 lines 56 – 62); and

for private data forming a complete character or image, repeatedly inserting portions of said complete character or image when indicated by said synchronization pulses in said sequencing pattern until all portions of said complete character or image are inserted in said data signal (Coteus Column 3 lines 10 – 16 and 45 – 51),

whereby display of said data signal, as viewed by said active glasses synchronized with said visual interface according to said sequencing pattern is a strobe display of said complete character or image (Coteus Column 2 lines 59 – 67).

Claim 29 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer

program for secure entry of a authorizing data in a publicly positioned device, wherein said step of opening and closing said shuttered display comprises the step of, responsive to synchronization pulses in said sequencing pattern, opening and closing said shuttered display (Coteus Column 6 lines 43 – 62).

Claim 31 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said sequencing pattern corresponds to alternating displays of said private data and said masking data (Coteus Column 3 lines 45 – 51).

Claim 32 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said sequencing pattern corresponds to combined left eye/right images of said private data (Coteus Column 2 lines 62 – Column 3 line 16).

Claim 33 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said masking data is a fill pattern (Coteus Column 3 lines 34 – 40 and 55 – 59).

Claim 34 is rejected as applied above in rejecting claim 25. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said establishing step comprises the step of:

connecting said user to a telephone operator system through said telephone interface, said prompts audibly provided by said telephone operator system to said user through said telephone interface (Column 5 lines 15 – 18).

Claim 12 is rejected as applied above in rejecting claim 8. Furthermore, Naik teaches and describes a method for secure entry of a authorizing data in a publicly positioned device, wherein said step of opening and closing said shuttered display comprises the steps of:

decoding said encoded sequencing pattern (Column 5 lines 28 – 32 and Column 6 lines 25 – 34) ; and

responsive to said synchronization pulses in said sequencing pattern , opening and closing said shuttered display (Coteus Column 2 lines 3 – 13).

Claim 30 is rejected as applied above in rejecting claim 26. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said step of opening and closing said shuttered display comprises the steps of:

decoding said encoded sequencing pattern (Column 5 lines 28 – 32 and Column 6 lines 25 – 34); and

responsive to said synchronization pulses in said sequencing pattern , opening and closing said shuttered display (Coteus Column 2 lines 3 – 13).

Claim 35 is rejected as applied above in rejecting claim 34. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said telephone operator system is an interactive voice response ("IVR") system (Column lines Column 6 lines 33 – 53).

Claim 36 is rejected as applied above in rejecting claim 34. Furthermore, Naik teaches and describes, a machine readable storage, having stored thereon a computer program for secure entry of a authorizing data in a publicly positioned device, wherein said telephone operator system is a human telephone operator. It is well known in the art that the authentication devices are equipped with hardware to allow a query-response type of authentication scheme to be used or to provide with an audio interface, are used to authenticate a device or an entity to communicate with the user to be equipped with both human telephone operator or with machine readable verification systems (Column 4 line 27 – Column 5 line 47).

***Conclusion***

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy

November 26, 2004.

EMMANUEL L. MOISE
PRIMARY EXAMINER